UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/915,628	07/26/2001	Bryan M. Willman	2721	6471

7590 12/21/2004

LAW OFFICES OF ALBERT S. MICHALIK, PLLC
704 228th AVENUE NE
SUITE 193
SAMMAAMISH, WA 98074

EXAMINER	
TANG, KENNETH	

ART UNIT	PAPER NUMBER
2127	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Applicati n No.	Applicant(s)	
	09/915,628	WILLMAN, BRYAN M.	
	Examin r	Art Unit	
	Kenneth Tang	2127	

-- Th MAILING DATE of this communication appears on th cover she t with the corr spond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 8/31/01.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-77 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-77 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-77 are presented for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-77 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention:

a. In claim 1, "a map" in line 5 is indefinite because it is not made explicitly clear in the claim language whether or not this is the same thing as "a first memory map" (3-4).

b. In claim 31, it is unclear whether the claims are independent or dependent claims. As is, computer-readable medium claims should not depend from computer-system claims. Claim 31 is required to be put into independent form.

c. In claim 32, "a protection mechanism" is indefinite because it is not made clear in the claim language what is being protected.

d. Claim 32 recites the limitations "the thread " in lines 3 and 13. There is insufficient antecedent basis for this limitation in the claim. It is also unclear whether "the thread" is only singular or could be plural by having at least one thread.

e. In claim 64, "first and second address maps" is indefinite because it is not made explicitly clear in the claim language whether or not this is the same thing as a "first and second memory map";

f. In claim 64, "changing the first address map to the second address map" (lines 20-21) is indefinite because it is unclear whether addresses or maps are being changed. In addition, it is unclear whether or not the first and address is a virtual address and physical address.

g. In claim 69, it is unclear whether the claims are independent or dependent claims. As is, computer-readable medium claims should not depend from computer method claims. Claim 69 is required to be put into independent form.

h. In claim 70, "switching" and "returning" is indefinite because it is not made explicitly clear in the claim language whether the map or the address is being switched and returned.

i. Claim 70 recites the limitations "the second map" and "the first map" in lines 9 and 11, respectively. There is insufficient antecedent basis for this limitation in the claim. In addition, it is unclear whether or not the first and second maps have any relation with the first address map and the second address map.

j. Claims 74 and 75 recite the limitation "third maps" in lines 2 and 7, respectively. There is insufficient antecedent basis for this limitation in the claim.

k. In claim 76, "each of the maps" (line 11) is indefinite because it is not made explicitly clear whether there are 2 or 3 maps that are being mapped.

l. In claim 77, it is unclear whether the claims are independent or dependent claims. As is, computer-executable instructions claims should not depend from computer method claims. Claim 77 is required to be put into independent form.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5, 7-34, and 36-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Magee et al. (hereinafter Magee) (US 5,729,710) in view of Williams (US 6,304,973 B1).

4. As to claim 1, Magee teaches in a computer-system, a method comprising:

receiving a request via a process thread having a first memory map associated therewith *(col. 18, lines 28-44)*;

Magee also teaches various privilege levels with maps *(col. 15, lines 10-34, col. 18, lines 43-44, col. 9, lines 40-56, col. 33, lines53-61)*. Magee fails to explicitly teach changing maps, performing the map change to associate a second memory map with the process thread, the second memory map providing different memory access with respect to the first memory map; and restoring the privilege level to a level that does not allow a map change. However, Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems *(col. 26, lines 18-26)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of teach changing maps, performing the map change to associate a second memory map with the process thread, the second memory map providing different memory access with respect to the first memory map; and restoring the

privilege level to a level that does not allow a map change to the existing system of Magee in order to increase the security and integrity of the system *(col. 26, lines 18-26)*.

5. As to claim 2, Magee teaches wherein receiving a request comprises receiving an application programming interface call at an operating system component *(col. 7, lines 11-22)*.

6. As to claim 3, Magee teaches wherein receiving a request comprises, receiving an operating system a call from a kernel mode component *(col. 21, lines 63-67)*.

7. As to claim 4, Magee teaches wherein the kernel mode component comprises an installable driver *(col. 6, lines 64-67)*.

8. As to claim 5, Magee teaches wherein changing a privilege level comprises calling a call gate *(col. 67, table 14)*.

9. As to claim 7, Magee teaches wherein performing the map change comprises writing a register *(col. 3, lines 11-13)*.

10. As to claim 8, Magee teaches wherein the second memory map accesses protected memory, and further comprising, executing trusted code while the second memory map is associated with the process thread *(col. 9, lines 63-67 through col. 10, lines 1-6, col. 14, lines 53-63)*.

11. As to claim 9, Magee teaches performing a second map change to re-associate the first map with the process thread *(col. 4, lines 64-67 through col. 5, lines 1-25)*.

12. As to claim 10, Magee teaches wherein executing trusted code includes entering function predefined entry point *(col. 14, lines 53-63, col. 3, lines 29-31)*.

13. As to claim 11, Magee teaches wherein entering the function comprises making an application programming interface call *(col. 7, lines 11-22)*.

14. As to claim 12, Magee teaches wherein the function allocates memory *(col. 17, line 60)*.

15. As to claim 13, Magee teaches wherein the function deallocates memory *(col. 17, line 60)*.

16. As to claim 14, Magee teaches wherein the function allocates an object *(col. 17, line 60)*.

17. As to claim 15, Magee teaches wherein the object comprises a handle *(col. 30, line 37)*.

18. As to claim 16, Magee teaches wherein the object comprises a synchronization objects *(col. 39, lines 17-58)*.

19. As to claim 17, Magee teaches wherein the object comprises a process *(col. 1, lines 34-37)*.

20. As to claim 18, Magee teaches wherein the object comprises threads *(col. 10, lines 54-67)*.

21. As to claim 19, Magee teaches wherein the function performs a trust-privileged operation *(col. 14, lines 53-67)*.

22. As to claim 20, Magee teaches wherein the trust-privileged operation comprises signaling a synchronization object *(col. 39, lines 17-58)*.

23. As to claim 21, Magee teaches wherein the trust-privileged operation comprises deleting a timer *(col. 19, lines 50-51, col. 13, lines 23-43)*.

24. As to claim 22, Magee teaches wherein the trust-privileged operation comprises closing a handle *(col. 30, line 37)*.

25. As to claim 23, Magee fails to explicitly teach wherein the first and second memory maps each include a mapping that maps virtual memory address to a physical memory address that is larger than the largest possible virtual memory address that an entity is allowed to address. However, this is obvious to one of ordinary skill in the art because a memory location larger than

the largest possible virtual memory address is needed because there is no longer room in the virtual memory addresses.

26. As to claim 24, Magee teaches wherein the virtual memory address that maps to a physical memory address that is larger is in user mode addressable space *(col. 9, lines 40-56)*.

27. As to claim 25, Magee teaches wherein the first and second memory maps each include a mapping that maps a virtual memory address to a physical memory address the same *(col. 3, lines 1-14)*.

28. As to claim 26, Magee teaches wherein the physical memory address that is the same in kernel mode addressable space *(col. 22, lines 51-57)*.

29. As to claim 27, it is rejected for the same reasons as stated in the rejections of claims 24-26.

30. As to claim 28, Magee teaches wherein the first and second memory maps each map a virtual memory address to a physical memory address that is common to both maps *(col. 3, lines 1-14)*.

31. As to claim 29, Magee teaches wherein the second map maps memory that is invalid in the first map *(col. 61, Table 8 and col. 63, table 11, and col. 47, lines 14-20)*.

32. As to claim 30, Magee teaches wherein the second map maps to has different access rights the first map *(col. 18, lines 29-44, col. 47, lines 14-20)*.

33. As to claim 31, it is rejected for the same reasons as stated in the rejections of claim 1.

34. As to claim 32, Magee teaches in a computing device: a system comprising:

a process having least one thread *(col. 20, lines 53-56, col. 3, lines 1-14)*;

a first memory map associated with the thread and having data therein that maps virtual memory addresses to physical memory *(col. 9, lines 40-56)*;

a second memory map having data therein that maps virtual memory addresses physical memory, the second memory map providing different memory access with respect to the first memory map *(col. 9, lines 40-56 and col. 18, lines 43-44)*;

a protection mechanism, the protection mechanism configured to allow changing of a map *(col. 33, lines 55-60, col. 15, lines 10-34, col. 18, lines 28-44)*; and

Magee teaches having a trusted server *(col. 24, lines 6-14)* but fails to explicitly teach trusted code configured invoke the protection mechanism to change the thread from being associated with the first map to be being associated with the second map. However, Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems *(col. 26, lines 18-26)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of switching to trusted and non-trusted mappings to

the existing system of Magee in order to increase the security and integrity of the system *(col. 26, lines 18-26)*.

35. As to claim 33, Magee teaches wherein the second memory map has more access rights to virtual memory addresses than the first memory map *(col. 14, lines 53-63, col. 15, lines 10-33)*.

36. As to claim 34, Magee teaches wherein protection mechanism comprises a call gate configured to change privilege levels *(col. 67, table 14)*.

37. As to claim 36, Magee teaches wherein the trusted code further includes a function *(col. 2, lines 48-50)*.

38. As to claim 37, Magee teaches wherein the function allocates memory to the process *(col. 17, line 60)*.

39. As to claim 38, Magee teaches wherein the function deallocates memory *(col. 17, line 60)*.

40. As to claim 39, Magee teaches wherein the function allocates an object *(col. 17, line 60)*.

41. As to claim 40, Magee teaches wherein the object comprises handle *(col. 30, line 37)*.

42. As to claim 41, Magee teaches wherein the object comprises synchronization objects *(col. 39, lines 17-58)*.

43. As to claim 42, Magee teaches wherein the object comprises a process *(col. 1, lines 34-37)*.

44. As to claim 43, Magee teaches wherein the object comprises a threads *(col. 10, lines 54-67)*.

45. As to claim 44, Magee teaches wherein the function performs a trust-privileged operation *(col. 14, lines 53-67)*.

46. As to claim 45, Magee teaches wherein the trust-privileged operation comprises signaling a synchronization object *(col. 39, lines 17-58)*.

47. As to claim 46, Magee teaches wherein the trust-privileged operation comprises deleting a timer *(col. 19, lines 50-51, col. 13, lines 23-43)*.

48. As to claim 47, Magee teaches wherein the trust-privileged comprises closing a handle *(col. 30, line 37)*.

49. As to claim 48, Magee teaches wherein only the trusted code is executed while the second memory map is in use *(col. 9, lines 63-67 through col. 10, lines 1-6, col. 14, lines 53-63)*.

50. As to claim 49, Magee teaches wherein the trusted code executes in response to from the process *(col. 21, lines 63-67)*.

51. As to claim 50, Magee teaches wherein the trusted code comprises an operating system component, and wherein the trusted code executes in response to an application interface call from the process an operating programming system component *(col. 7, lines 11-22)*.

52. As to claim 51, Magee teaches wherein the protection mechanism comprises a call gate *(col. 67, table 14)*.

53. As to claim 52, Magee teaches wherein the trusted code changes the thread from being associated with the first map to be being associated with the second map by writing to a register *(col. 3, lines 11-13)*.

54. As to claim 53, Magee teaches wherein the trusted code changes the thread from being associated with the first map be being associated with the second map by instructing a hardware component to select a different subset a translation look-aside buffer *(col. 4, lines 64-67 through col. 5, lines 1-25)*.

55. As to claim 54, Magee teaches wherein the trusted code performs a second map change to re-associate the first map with the process thread, to not allow map changing *(col. 33, lines 55-60)*.

56. As to claim 55, Magee teaches wherein the protection mechanism changes a privilege level (changing rights) to not allow map changing *(col. 24, lines 56-59, col. 33, lines 55-60)*.

57. As to claim 56, Magee fails to explicitly teach wherein the first and second memory maps each include a mapping that maps a virtual memory address to a physical memory address that is larger than the largest possible virtual memory address that an entity is allowed to specify. However, this is obvious to one of ordinary skill in the art because a memory location larger than the largest possible virtual memory address is needed because there is no longer room in the virtual memory addresses.

58. As to claim 57, Magee teaches wherein the virtual memory address that maps to a physical memory address larger is in user mode addressable space *(col. 9, lines 40-56)*.

59. As to claim 58, Magee teaches wherein the first and second memory maps each include a mapping maps a virtual memory address to a physical memory address that is the same *(col. 3, lines 1-14)*.

60. As to claim 59, Magee teaches wherein the physical memory address that is the same is in kernel mode addressable space *(col. 22, lines 51-57)*.

61. As to claim 60, Magee teaches wherein the first and second memory maps each map a virtual memory address to a physical memory address that is common to both maps *(col. 3, lines 1-14)*.

62. As to claim 61, Magee teaches wherein the second map maps to memory that is invalid in the first map *(col. 61, Table 8 and col. 63, table 11, and col. 47, lines 14-20)*.

63. As to claim 62, Magee teaches wherein the second map maps to memory that has different access rights in the first map *(col. 18, lines 29-44, col. 47, lines 14-20)*.

64. As to claim 63, fails to explicitly teach teaches wherein the second map shares a mapping of some virtual addresses to physical addresses common to the first map, and includes another mapping of virtual addresses to the physical addresses that are not common to the first map. However, Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems *(col. 26, lines 18-26)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of switching to the second map prior to running a first set of untrusted code without switching process and returning to the first map after completion of the untrusted code to the existing system of Magee in order to increase the security and integrity of the system *(col. 26, lines 18-26)*.

65. As to claim 64, Magee teaches a computer-implemented method, comprising:

associating first and second address maps with a process *(col. 9, lines 40-56, col. 18, lines 43-44)*;

receiving a request from a thread process change from the first address map to the second address map *(col. 37, lines 40-67, col. 18, lines 28-44)*;

66. Magee fails to explicitly teach changing the first address map to the second address map. However, Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems *(col. 26, lines 18-26)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of switching to the second map prior to running a first set of untrusted code without switching process and returning to the first map after completion of the untrusted code to the existing system of Magee in order to increase the security and integrity of the system *(col. 26, lines 18-26)*. Magee also fails to explicitly teach using the mapping to access data at a physical memory location having a physical address that is larger than the largest possible virtual memory address. However, this is obvious to one of ordinary skill in the art because a memory location larger than the largest possible virtual memory address is needed because there is no longer room in the virtual memory addresses.

67. As to claim 65, Magee teaches wherein the first and second memory maps each map a virtual memory address to a physical memory address that is the same *(col. 3, lines 1-14)*.

68. As to claim 66, Magee teaches wherein each virtual memory address that maps a physical memory address that is larger is user mode addressable space, and wherein the physical memory address that is the same kernel mode addressable space *(col. 22, lines 51-57)*.

69. As to claim 67, Magee fails to explicitly teach having a third map but it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a third map to the system because it would provide for different privileges for security.

70. As to claim 68, Magee teaches wherein changing the first map the second map includes calling the operating system to switch the maps *(col. 21, lines 63-67)*.

71. As to claim 69, it is rejected for the same reasons as stated in the rejection of claim 64.

72. As to claim 70, Magee teaches a computer-implemented method, comprising:

associating first and second address maps with a process, wherein the second address map provides different memory access with respect to the first memory map *(col. 9, lines 40-56, col. 18, lines 43-44)*;

running trusted code with the first map *(col. 24, lines 6-14)*;

73. Magee fails to explicitly teach switching to the second map prior to running a first set of untrusted code without switching process and returning to the first map after completion of the untrusted code. However, Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems *(col. 26, lines 18-26)*. It would have been obvious to

one of ordinary skill in the art at the time the invention was made to combine the feature of switching to the second map prior to running a first set of untrusted code without switching process and returning to the first map after completion of the untrusted code to the existing system of Magee in order to increase the security and integrity of the system *(col. 26, lines 18-26)*.

74. As to claim 71, Magee teaches wherein switching to the second map includes calling the operating system to switch the maps *(col. 21, lines 63-67)*.

75. As to claim 72, Magee teaches wherein the first and second maps map to at least one physical address that is the same *(col. 3, lines 1-14)*.

76. As to claim 73, Magee teaches further comprising switching to a third map prior to running a second set of untrusted code without switching the process *(col. 3, lines 1-14)*. Magee fails to explicitly teach having a third map but it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a third map to the system because it would provide for different privileges for security.

77. As to claim 74, it is rejected for the same reasons as stated in the rejection of claim 73. In addition, Magee teaches mapping to at least one physical address that is the same *(col. 3, lines 1-14)*.

78. As to claim 75, it is rejected for the same reasons as stated in the rejection of claim 73. In addition, Magee teaches mapping to at least one physical address that is the same *(col. 3, lines 1-14)*.

79. As to claim 76, Magee teaches wherein each of the maps map to at least one physical address that is the same *(col. 3, lines 1-14)*.

80. As to claim 77, it is rejected for the same reasons as stated in the rejection of claim 70.

81. Claims 6 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Magee et al. (hereinafter Magee) (US 5,729,710) in view of Williams (US 6,304,973 B1), and further in view of Gulsen (US 5,727,211).

82. As to claim 6, Magee and Williams fails to explicitly teach wherein changing a privilege level comprises changing to a ring 0 privilege level. However, Gulsen teaches using a ring 0 level *(col. 6, lines 23-36 and 47-55)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of a ring 0 level to the existing system because this provides a protection layer *(col. 6, lines 23-36 and 47-55)*.

83. As to claim 35, Magee and Williams fails to explicitly teach wherein the trusted code includes a thunk configured to re-vector directed to one set of code to another set of code.

However, Gulsen teaches thunking to be a standard process by which 16-bit 80x86 code modifies certain process calling sequences to allow it call 32-bit code *(col. 4, lines 56-60)*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the feature of thunking to the existing system because it would allow reconstructing part of data structures for parameter passing and return *(col. 4, lines 56-60)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Tang whose telephone number is (571) 272-3772. The examiner can normally be reached on 8:30AM - 6:00PM, Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MENG-AI T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kt
12/10/04